شرکت اپل که به‌عنوان یکی از مدافعان بلامنازع امنیت و حریم خصوصی معرفی می‌شود، به درخواست دادگاه هر اطلاعاتی حتی محتوای پیام‌ها را در اختیار نهاد دولتی اف‌بی‌آی قرار می‌دهد

در بیشتر کشورها حق دسترسی به اطلاعات پیام‌ها در صورتی که فردی مظنون به فعالیت تروریستی یا تعرض به کودکان و موارد مشابه باشد برای دادگاه محفوظ است

کلیک ماجرای همکاری پیام‌رسان‌ها با اف‌بی‌آی آمریکا را بررسی می‌کند

رقابت در همکاری با FBI

عباس ملک‌حسینی
ایده‌پرداز در زمینه تجارت الکترونیک

بنیاد مرزهای الکترونیکی که از سال ۱۹۹۰ در زمینه آزادی اینترنت ،کنترل شرکت‌ها و دولت‌ها بر اینترنت فعالیت می‌کند به‌تازگی گزارش جدیدی از حق دسترسی پیام‌رسان‌ها برای اف‌بی‌آی ایالات‌متحده منتشر کرده است. این گزارش با اتکا به یک سند درز کرده از اف‌بی‌آی تنظیم می‌شود و اعلام می‌کند امنیت سرویس‌های پیام‌رسان واتس‌اپ و آی‌مسیج اپل کمترین در میان پیام‌رسان‌های موجود است.به عبارتی دیگر این سند نشان می‌دهد واتس‌اپ، فیسبوک و آی مسیج اپل بیشترین حجم اطلاعات را در اختیار این سازمان قرار می‌دهند همچنین می‌تواند چنین اطلاعاتی را به‌طور قانونی از هر برنامه پیام‌رسانی به دست آورد. این سند اولین بار توسط کاربر simplefilmreviews در سایت ردیت منتشر شد.

همان‌طور که در تصویر پایین صفحه مشاهده می‌کنید، واتس‌اپ اطلاعات مختلفی را در اختیار اف‌بی‌آی می‌گذارد؛ مخاطبان شما، اطلاعات هویتی، زمان ارسال و دریافت پیام، زمان ثبت‌نام، اطلاعات فرستنده و گیرنده پیام‌ها. با این حال محتوای پیام و کلید ردوبدل شده در اختیار نهادی قرار نمی‌گیرد، چراکه خود واتس‌اپ به کلید انکریپشن و رمزنگاری پیام‌ها نیز دسترسی ندارد. اما شرایط زمانی پیچیده می‌شود که شما اطلاعات واتس‌اپ را در سرویس معروف iCLoud از شرکت اپل ذخیره و پشتیبان‌گیری کنید. ماجرا در اپل کمی متفاوت‌تر از فیسبوک است. شرکت اپل به‌عنوان یکی از مدافعان بلامنازع امنیت و حریم خصوصی معرفی می‌شود اما طبق این سند که اوایل سال ۲۰۲۱ تنظیم شده است، شرکت اپل به درخواست دادگاه هر اطلاعاتی حتی محتوای پیام‌ها را در اختیار نهاد دولتی قرار می‌دهد. همچنین اگر واتس‌اپ اطلاعاتی به دولت ندهد اما چون بک آپ اطلاعات در iCloud است، اپل موظف می‌شود آنها را در اختیار اف‌بی‌آی قرار دهد. اف‌بی‌آی می‌تواند داده‌های آدرس بوک (Address book) را هم از هدف و هم از مخاطبان آنها بگیرد. این سازمان حتی می‌تواند منبع و مقصد پیام‌های ارسال شده از برنامه را نیز ردیابی کند. به این معنا که اگر اطلاعات تماس موردنظر را ذخیره کرده باشید، آدرس بوک شما نیز در دسترس اف‌بی‌آی است تا بتواند در آن سرک بکشد.

اپلیکیشن‌های نفوذپذیر

اغلب اپلیکیشن‌ها اطلاعات مختلفی در سطوح گوناگون در اختیار دولت‌ها قرار می‌دهند به‌عنوان‌مثال پیام‌رسان تلگرام از کاربران، زمان ثبت‌نام، آی پی و شماره موبایل را دریافت می‌کند و طبیعتا به درخواست دادگاه برای موارد تروریستی و پس از بررسی توسط شرکت در اختیار دادگاه قرار می‌دهد. البته این اطلاعات صرفا به شماره موبایل، آی پی و زمان ثبت نام محدود می‌شود.

اپلیکیشن دیگر Threema است که خود را امن‌ترین پیام‌رسان معرفی می‌کند. این اپلیکیشن از ابتدا تمام پیام‌ها را در چند مرحله رمزنگاری می‌کند. حتی اطلاعات ثبت‌نام مانند شماره تلفن‌همراه و ایمیل نیز رمزنگاری می‌شود. با این حال شما برای فعالیت در تریما الزامی به وارد کردن شماره تلفن‌همراه یا ایمیل ندارید.

دیگر اپلیکیشن‌ها نیز به‌تناسب، دسترسی محدودی به دولت‌ها می‌دهند اما نکته کلیدی در این سند، پیام‌رسان اپل است چراکه این شرکت حریم خصوصی را اولویت اول خود قرار داده است.

آیا دولت‌ها حق دسترسی به اطلاعات پیام‌رسان‌ها را دارند؟

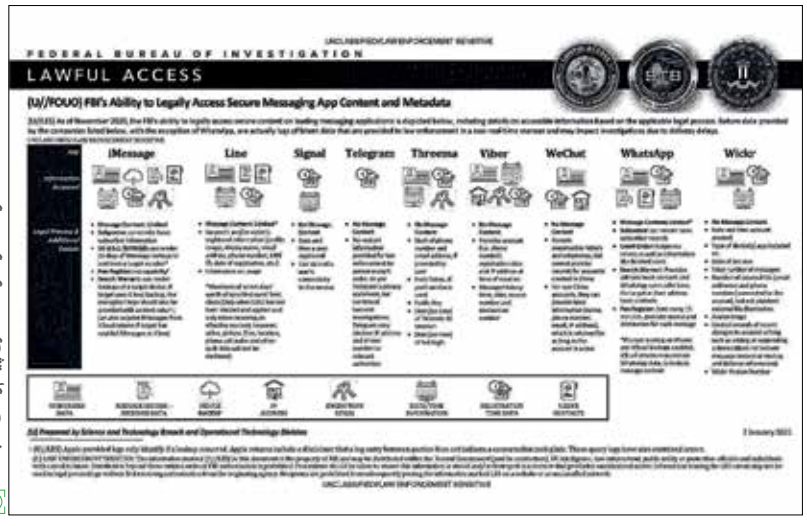
سؤال مهم همین است و هر کشوری بسته به شرایط خود، قوانین متفاوتی تعریف کرده است. به‌عنوان مثال در کشور ایران هیچ شرکت و سازمانی که در بستر اینترنت فعالیت می‌کند، حق حذف اطلاعات کاربران را ندارد. دسترسی به محتوای پیام‌ها و فعالیت کاربران موضوع دیگری است اما مسأله اصلی حریم خصوصی کاربران، اعتماد به شرکت‌ها و درنهایت دولت‌هاست.

در بیشتر کشورهای غربی، حق دسترسی به اطلاعات پیام‌ها در صورتی که فردی مظنون به فعالیت تروریستی یا تعرض به کودکان و موارد مشابه باشد برای دادگاه محفوظ است. با این حال برخی پیام‌رسان‌ها مثل سیگنال، تلگرام، تریما و حتی بخش محتوای پیامی در واتس‌اپ، از ابتدا دسترسی به چنین محتوایی را ناممکن کرده‌اند و حتی با حکم دادگاه، هیچ محتوایی از پیام‌ها را نمی‌توانند به دست بیاورند.

به این منظور بدافزارهایی مثل پگاسوس ساخته می‌شود که هدف خود را کشف محتوای این پیام‌ها برای دولت‌ها می‌داند، هرچند به نقض حریم خصوصی و به خطر انداختن جان کاربران متهم می‌شود.

کنترل بر محتوای پیام‌ها در اینترنت و فعالیت کاربران به‌سادگی امکان‌پذیر نیست. با این حال کاربران دوست دارند به‌جز خودشان و طرف مقابل، هیچ‌کس حرف آنها را نشنوند.

اگر واتس‌اپ اطلاعاتی به دولت ندهد اما چون بک‌آپ اطلاعات در iCloud است، اپل موظف می‌شود آنها را در اختیار اف‌بی‌آی قرار دهد



سند منتشر شده از نحوه همکاری پیام‌رسان‌ها با FBI

چه اطلاعاتی از ما دریافت می‌شود؟

آخرین نسخه‌های اندروید و iOS تقریبا دسترسی به بخش‌های مختلف را در اختیار کاربران می‌گذارند. همچنین هنگام نصب هر اپلیکیشنی شما با موارد دسترسی مواجه می‌شوید.

اطلاعاتی مانند مدل گوشی، نام شما، حساب کاربری جیمیل یا اپل آی دی، شماره موبایل ثبت‌شده در دستگاه و تاریخ تولد از رایج‌ترین مواردی است که تقریبا هر اپلیکیشنی به آنها دسترسی دارد.

اما اطلاعات مهم‌تر مانند دسترسی به دوربین، مخاطبان، آخرین تماس‌ها دسترسی به میکروفن، تصاویر گالری و ویدئوها، موقعیت جغرافیایی، پیام‌های اطلاع‌رسانی، پیامک‌ها و موارد این‌چنینی در اختیار کاربر است. درواقع اپلیکیشن برای کار کردن به این اطلاعات نیاز دارد و اگر دسترسی کامل به شما ندهد، بخشی از خدمات کامل نمی‌شود.

برای نمونه شما می‌توانید واتس‌اپ را بدون دسترسی مخاطبان نصب کنید اما در این حالت امکان پیدا کردن هیچ‌یک از مخاطبان گوشی خود را نخواهید داشت یا برای اشتراک‌گذاری زنده موقعیت جغرافیایی، خود اپلیکیشن نیاز به این دسترسی دارد.

نکته‌ای که در این گزارش مطرح‌شده ، حجم بسیار بالای اطلاعات دریافتی و همچنین اشتراک‌گذاری آنها با دولت است.

در واقع این اطلاعات شما که با اپلیکیشن‌ها به اشتراک گذاشته می‌شود آیا پس از مدتی حذف می‌شود یا با حذف حساب شما از بین می‌رود یا تا ابد در اختیار آنها باقی می‌ماند؟